CHAPTER

16

TROUBLESHOOTING WINDOWS 2000

After reading this chapter and completing the exercises, you will be able to:

- Collect documentation about your systems to aid in troubleshooting and preventing problems
- Review common-sense approaches to troubleshooting
- Troubleshoot general problems with Windows 2000
- Use some of the troubleshooting tools of Windows 2000

Windows 2000 troubleshooting is an important and vast area. In this chapter, you learn how to detect, isolate, and eliminate problems with installation, printing, remote access, the network, disks, and other aspects of a Windows 2000 system.

In addition to the techniques discussed in this chapter, important troubleshooting options and features of Windows 2000 have been covered in earlier chapters. The Registry is a common location in which problems occur as well as a source for implementing solutions. Working with the Registry is discussed in Chapter 13. The Windows 2000 boot process is often a source of problems. These problems and their respective solutions are discussed in Chapter 14. Catastrophic events, virus infections, or simple hardware failure can leave you without a functioning system. Disaster recovery and backups are discussed in Chapter 15. Keep the troubleshooting advice provided in the previous three chapters in mind when attempting to prevent and resolve problems involving Windows 2000.

General Principles of Troubleshooting

When trouble arises in Windows 2000, you need to take action to resolve the issue as quickly as possible. Troubleshooting is the art and science of systematically eliminating problems in a computer system. Although troubleshooting may sound exciting, in reality it is usually a fairly tedious process. In the following sections, we outline some procedures and common-sense guidelines that should improve your troubleshooting skills and help you keep downtime to a minimum.

Collecting Information

The first rule of troubleshooting is that you can never have too much information. In fact, information is your best weapon, not just for resolving problems, but also for preventing them in the first place. Useful information typically falls into three areas: details about your system (hardware and software), details about previous troubleshooting, maintenance, and configuration activities, and details about the current problem.

Collecting information about your system's hardware and software is a preventive maintenance task. It requires that you gather all pertinent information and keep it in an accessible form and location. We call this collection a **computer information file (CIF)**. A good CIF provides a detailed collection of all information related to the hardware and software products that compose your computer (and even your entire network). A CIF is not just a single file, but an ever-expanding accumulation of data sheets sorted into related groupings. Your CIF should be stored in a protected area (such as a safe or fireproof vault) that can be accessed in the event of an emergency (a bank's safety deposit box won't allow you to get at the information at three o'clock in the morning). Obviously, constructing a CIF from scratch is a lengthy process, but one that will be rewarded with averted problems, easy reconfigurations, or simplified replacement of failed components.

Some of the important items to include in your CIF are:

- Platform, type, brand, and model number of each component
- Complete manufacturer specifications
- Configuration settings, including jumpers and DIP switches, plus what each setting means, including IRQs, DMA addresses, memory base addresses, and port assignments
- Manuals, users' guides, or configuration sheets
- Version of BIOS, driver software, patches, fixes, etc., with floppy copies
- Printed and floppy copies of all parameter and initialization files
- Detailed directory structure printout
- Name and version of all software
- Network-assigned names, locations, and addresses

- Status of empty ports, upgrade options, or expansion capabilities
- System requirements, such as the manufacturer's listed minimum requirements for its operating system, driver, applications, and hardware
- Warranty information, such as service phone numbers and e-mail addresses
- Complete technical support contact information, including support Web site URLs
- Error log with detailed and dated entries of problems and solutions
- Date and location of last complete backup, and other backup items
- Network layout and cabling map
- Copies of all software, operating system, and driver installation or source CDs and/or diskettes

Each of these items should be dated and initialed. However, your CIF is not complete with only hardware and software details. You should also include the nonphysical characteristics of your system, such as:

- Information services present, such as Web, FTP, e-mail, newsgroups, and message boards
- Important productivity services, such as productivity suites (Microsoft Office), collaboration utilities, whiteboard applications, and video conferencing products
- Plans for future service deployment
- A mapping or listing of related hardware and software for each service or application present on the system
- Structure of authorized access and security measures
- Training schedule
- Maintenance schedule
- Backup schedule
- Contact information for all system administrators
- Personnel organization or management hierarchy
- Workgroup arrangements
- Online data storage locations
- In-house content and delivery conventions
- Authorship rights and restrictions
- Troubleshooting procedures

Neither of these lists is exhaustive. As you operate and maintain your systems you'll discover other important items to add to the CIF.

Remember, if you don't document it, then you won't be able to find it when you really need it. A good way to keep the CIF current is to add, remove, or modify its contents each time you make a system modification. Performing a quarterly or semiannual audit of the CIF is not a bad idea, either.

It is essential that the content of the CIF be thorough and up to date. Without thorough, specific, and accurate information about the products, configuration, setup, and problems associated with your network, the CIF will be useless. Keep in mind that the time you spend organizing your CIF will reduce the time required to locate information when you really need it. It is wise to create a correlation system so that you can easily associate items in the CIF with the actual component, using, for example, an alphanumeric labeling system. For instructions on how to create a CIF, see Hands-on Project 16-2.

We recommend maintaining both a printed/written version and an electronic version of the CIF. Every time a change, update, or correction occurs, it should be documented in the electronic version, and a printout made and stored. Murphy's Law guarantees that the moment you need your electronic data most is when your system will not function.

Common-Sense Troubleshooting Guidelines

When problems occur, you would like to be at your sharpest. However, by a corollary to Murphy's Law, you'll probably find that problems tend to occur when you are stressed, when you are short on time, or when it is just generally inconvenient. If you take the time to keep your CIF up to date and keep the following common-sense guidelines in mind, you'll take some of the headache out of troubleshooting, and be better prepared to resolve problems quickly.

- *Be patient:* Anger, frustration, hostility, and frantic impatience usually cause problems to intensify rather than dissipate.
- *Be familiar with your system's hardware and software:* If you don't know what the normal baselines for your system are, you may not know when a problem is solved or when new problems surface. (See Chapter 11 for information on creating baselines.)
- *Attempt to isolate the problem:* When possible, eliminate segments or components that are functioning properly, thus narrowing the range of suspected problem sources.
- *Divide and conquer:* Disconnect, one at a time, as many nonessential devices as possible, to narrow down the investigation.
- *Eliminate suspects:* Move suspect components, such as printers, monitors, mice, or keyboards, to a known good computer to see if they work in the new location.
- *Undo the most recent change:* If you have recently made a change to your system, the simplest fix may be to undo the most recent alteration, upgrade, or change.

- *Investigate the most common points of failure:* The most active or sensitive components are the most common points of failure—these include hard drives, cables, and connectors.
- *Recheck items that have caused problems before:* As the old axiom goes, "history repeats itself" (and usually right in your own backyard).
- *Try the easy and quick fix first:* Try the easy fixes before moving on to the more time-consuming, difficult, or even destructive measures.
- *Let the fault guide you:* The adage, "Where there is smoke, there is fire" applies to computer problems as well as to life in general. Investigate components and system areas associated with the suspected fault.
- *Make changes one at a time:* A step-by-step process enables you to clearly distinguish the solution when you stumble upon it.
- *Repeat the failure:* Often, being able to repeat an error is the only way to locate it. Transient and inconsistent faults are difficult to find due to their "now you see it, now you don't" nature.
- *Keep a detailed log of errors and attempted solutions:* Keep track of everything you do (both successful and failed attempts). This will prove an invaluable resource when an error occurs again on the same or a different system, or when the same system experiences a related problem.
- *Learn from mistakes (your own and others'):* Studying the mistakes of others can save you from making the same mistakes; a wise person looks at failures as aids to finding a better solution.
- *Experiment:* Try similar tasks to see if a pattern develops.

There is probably not much in this list of common-sense items that you don't already know. The hardest part is remembering them when you are in the heat of a crisis.

TROUBLESHOOTING TOOLS

Becoming familiar with the repair and troubleshooting tools native to Windows 2000 can save you countless hours in troubleshooting. In the next sections, we detail how to use the Event Viewer and the Computer Management tools.

Event Viewer

The **Event Viewer** is used to view system messages regarding the failure or success of various key occurrences within the Windows 2000 environment (see Figure 16-1). The items recorded in the Event Viewer logs inform you of system drivers or service failures as well as security problems or ill-behaved applications (see Hands-on Project 16-1).

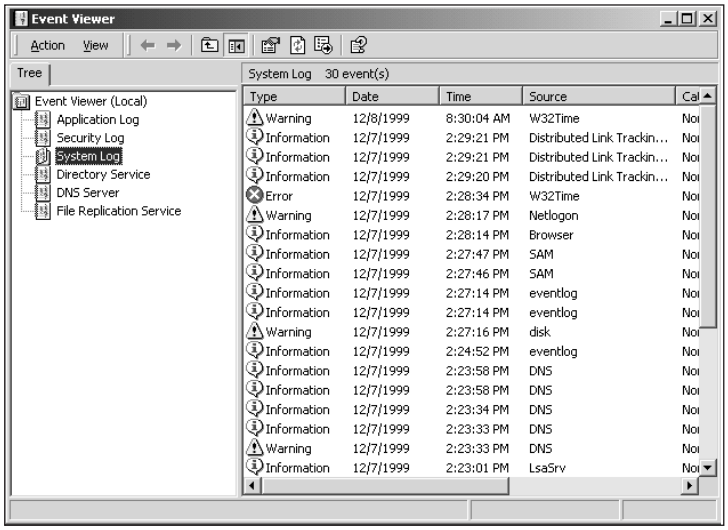

Figure 16-1 Event Viewer with System Log selected

Located in the Administrative Tools section of the Control Panel and Start menu, the Event Viewer is used to view the logs created automatically by Windows 2000. These logs are:

- ***System log***: The System log records information and alerts related to the Windows 2000 internal processes, including hardware and operating system errors, warnings, and general information messages.
- ***Security log***: The Security log records security-related events, including audit events of failed logons, user-right alterations, and attempted object access without sufficient permission.
- ***Application log***: The Application log records application events, alerts, and system messages.

Each log records a different type of event, but all the logs collect the same metainformation about each event: date, time, source, category, event, user ID, and computer. Each logged event (Figure 16-2 shows the properties of a logged event) includes some level of detail about the error, ranging from an error code number to a detailed description with a memory HEX buffer capture. For example, Figure 16-2 shows an event detail involving a time problem from a domain controller; it states how to rectify the problem with a command, and includes the HEX result that caused the problem (however, the HEX information listed is of no help to you for this specific problem). Most system errors, including Stop errors that result in the blue screen, are recorded in the System log. This allows you to review the time and circumstances of a system failure. The details in the Event Viewer can often be used as evidence in

your search for the cause of a problem. However, the event details offer little information on how to actually resolve a problem.

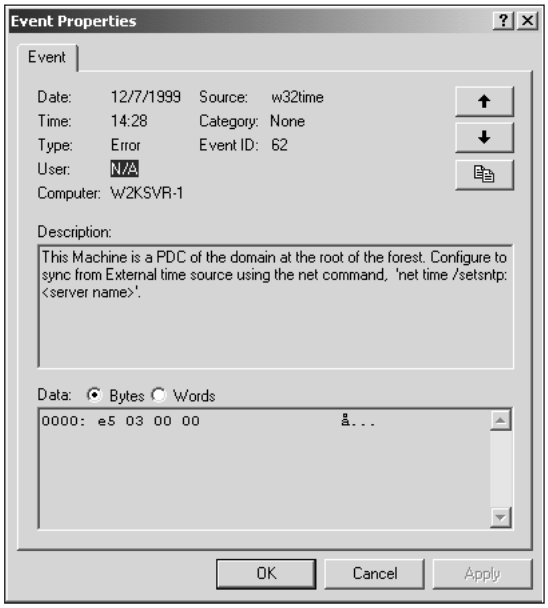

Figure 16-2 Event Viewer event detail

Computer Management Tool

Windows 2000 combines the robustness of Windows NT with the ease of configuration of Windows 98 Plug and Play. An added advancement in hardware support, and a useful side effect of Plug and Play, is the simplicity of the troubleshooting tools for nearly every aspect of Windows 2000. Most of these tools are collected into a single interface called the Computer Management tool (see Figure 16-3), found in the Administrative Tools section of the Control Panel and Start menu.

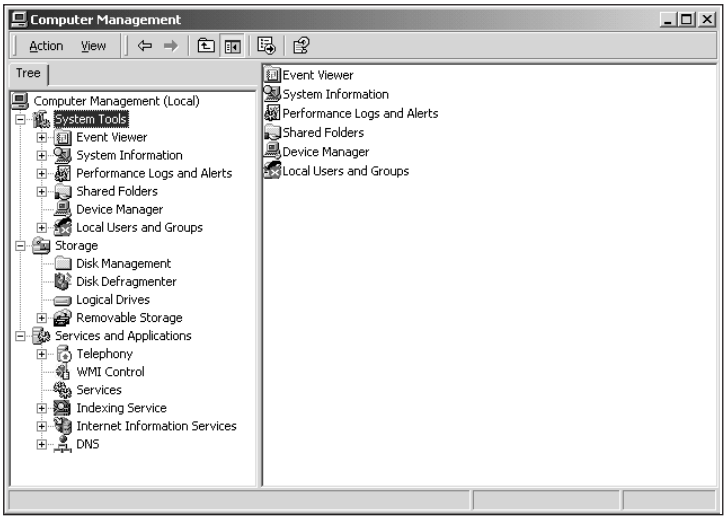

Figure 16-3 Computer Management

The Computer Management tool includes many tools similar to those in Windows NT and Windows 98, as well as several new utilities. Grouping all of these utilities in a single interface makes locating and resolving problems on key system components easier (see Hands-on Project 16-3). The Computer Management console is divided into three sections: System Tools, Storage, and Services and Applications. The System Tools section contains six tools:

- *Event Viewer:* Used to view system messages regarding the failure and/or success of various key occurrences within the Windows 2000 environment. Details about system errors, security issues, and application activities are recorded in the logs viewed through the Event Viewer. See the description of the Event Viewer earlier in this chapter. Hands-on Project 16-1 shows you how to use the Event Viewer.
- *System Information:* Used to gain configuration information and status summaries for the computer and operating system environment. You can quickly discover information such as system model numbers, free IRQs, sharing conflicts, and component configurations. This tool is invaluable when attempting to add new hardware into your system. Hands-on Project 16-2 shows you one way to use this tool.
- *Performance Logs and Alerts:* Another means to access the performance monitoring tool of Windows 2000 (see Chapter 11 for examples and hands-on projects involving this tool).
- *Shared Folders:* Used to view the shared folders on the local system. This interface shows hidden shares, current sessions, and open files. This tool allows you to view and alter the share configuration settings for user limit, caching, and permissions.
- *Device Manager:* Used to view and alter current hardware configurations of all local devices. Details on how to use the Device Manager, examples, and hands-on projects for this tool are located in Chapter 3.

- *Local Users and Groups:* Used to create and manage local user accounts and groups. (This tool is disabled when Active Directory is present.) Details on how to use this tool, examples, and hands-on projects are located in Chapter 5.

The Storage section of Computer Management has four tools used to simplify storage device administration. Details on how to use the Storage tools, examples, and hands-on projects are located in Chapter 4.

- *Disk Management:* Used to view and alter the partitioning and volume configuration of hard drives.
- *Disk Defragmenter:* Improves the layout of stored data on drives by reassembling fragmented files and aggregating unused space.
- *Logical Drives:* Used to gain information about logical drives (that is, those which you've formatted and assigned drive letters to).
- *Removable Storage:* Used to manage removable media such as floppy disks, tapes, and Zip drives.

The Services and Applications section contains management controls for various installed and active services and applications. The actual contents of this section depend on what is installed on your system. Some of the common controls are:

- *Services:* For stopping and starting services as well as configuring the startup parameters for services (such as whether to launch when the system starts and if to employ a user account security context to launch the service). Hands-on Project 16-8 shows you one way to use this tool.
- *Indexing Service:* For defining the collection of documents indexed for searching by the Indexing Service. For information on using this tool, consult the *Windows 2000 Resource Kit*.
- *Internet Information Services:* For managing Internet services. For information on using this tool, consult the *Windows 2000 Resource Kit*.
- *DNS:* For managing the Domain Name Service. For information on using this tool, consult Chapter 7 and the *Windows 2000 Resource Kit*.

Troubleshooting Installation Problems

Unfortunately, the installation process of Windows 2000 is susceptible to several types of errors: media errors, domain controller communication difficulties, Stop message errors or being hung up on a blue screen, hardware problems, and dependency failures. The following list contains a short synopsis of each error type and possible solutions:

- *Media errors:* Media errors are problems with the distribution CD-ROM itself, the copy of the distribution files on a network drive, or the communications link between the installation and the distribution files. The only regularly successful solution to media errors is to switch media, for example, copying the files to a network drive, linking to a server's CD-ROM, or installing a CD-ROM on the workstation. If media errors are encountered, always restart the installation process from the beginning.

- *Domain controller communication difficulties:* Communication with the domain controller is crucial to some installations, especially when attempting to join a domain. Most often this problem is related to mistyping a name, password, domain name, etc., but network failures and offline domain controllers can be causes as well. Verify the viability of the domain controller directly and from other workstations (if applicable), and then check that there are no mistyped entries in the installation process.
- *Stop message errors or halting on the blue screen:* Using an incompatible or damaged driver controller is the most common cause of Stop messages and halting on the blue screen during installation. If any information is presented to you about an error, try to determine if the proper driver is being used. Otherwise, double-check that your hardware has the drivers required to operate under Windows 2000.
- *Hardware problems:* If you failed to verify your hardware with the HCL (hardware compatibility list), or if a physical defect has occurred in a previously operational device, very strange errors can surface. In such cases, replacing the device is the only viable solution. Before you go to that expense, however, double-check the installation and configuration of all devices within the computer.
- *Dependency failures:* The failure of a service or driver due to the failure of a foundation or prior service or driver is a dependency failure. An example of a dependency failure is the Server and Workstation services failing (see Hands-on Project 16-8) because the NIC fails to initialize properly. Often Windows 2000 will boot in spite of these errors, so check the Event log (see Hands-on Project 16-1) for more details (see Figure 16-4).

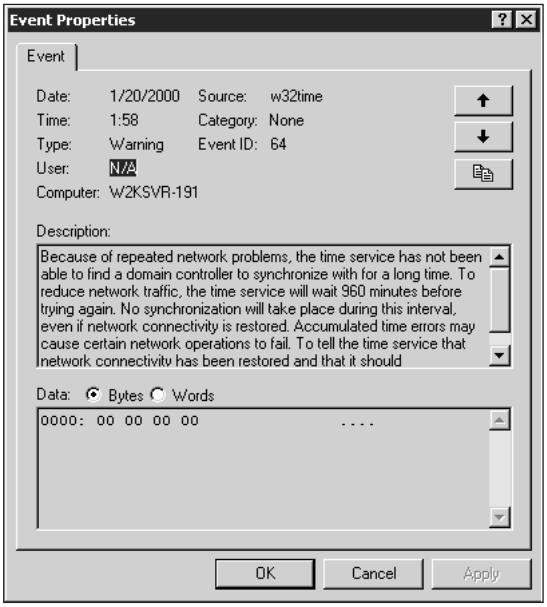

Figure 16-4 A dependency failure event detail from the System log of the Event Viewer

Just knowing about these installation problems can help you avoid them. Unfortunately, successfully installing Windows 2000 does not eliminate the possibility of further complications. Fortunately, Microsoft has included several troubleshooting tools that can help locate and eliminate most system failures (see the "Troubleshooting Tools" section earlier in this chapter).

Troubleshooting Printer Problems

Problems with network printers can often bring normal productive activity to a halt. Printer problems can occur anywhere from the power cable of the printer to the application attempting to print. Systematic elimination of possible points of failure is the only reliable method of eliminating printing errors. Here are some common and useful tips for troubleshooting printer problems:

- Check that the physical aspects of the printer—cable, power, paper, toner, and so on—are functional.
- Make sure the printer is plugged in and online. There is typically a light or an LCD message to indicate this. You may need to press the Reset button or the Online button to set or cycle the printer into online mode.
- Make sure the printer server for the printer is booted.
- Check the logical printer on both the client and server. Verify that they exist. Check their configuration parameters and settings. For details on logical printers and their multitude of controls, see Chapter 10.
- Check the print queue for stalled jobs (see Figure 16-5, which shows a stalled print job). If a print job does not otherwise have a status listing—such as waiting, paused, or printing—you can assume that it is stalled. The print queue is accessed by clicking the Start menu, selecting Settings, selecting Printers, then double-clicking on the icon for the printer.

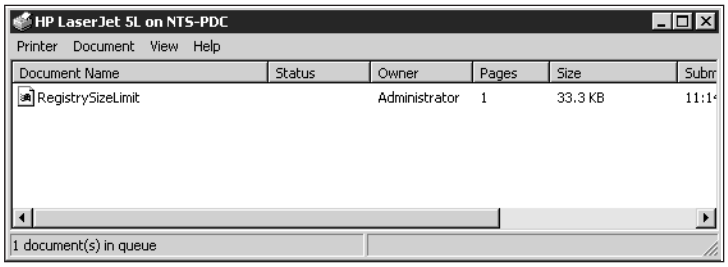

Figure 16-5 A printer queue

- Reinstall or update the printer driver to correct for a corrupt or incorrect print driver.
- Attempt to print from a different application or a different client.
- Attempt to print using Administrator access.

- Stop and restart the Print Spooler service, using the Services tool found via Computer Management (try Hands-on Project 16-4).
- Check the status and CPU usage of the Spoolsv.exe file, using the Task Manager (see Figure 16-6). If the spooler seems to be stalled by not receiving CPU time or is consuming most of the CPU, you should stop and restart the Spooler service.

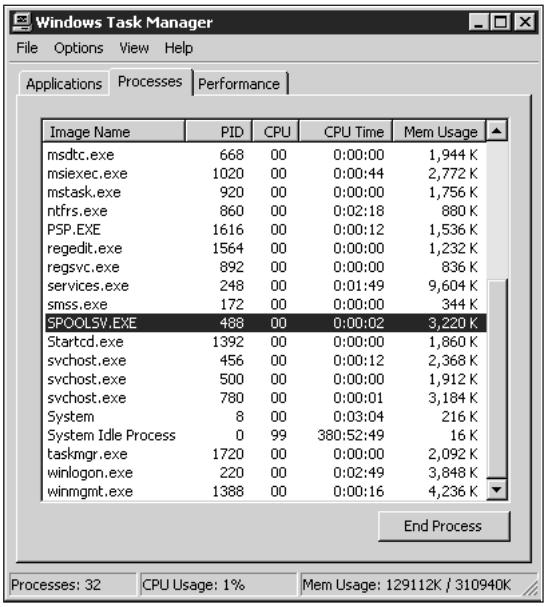

Figure 16-6 Task Manager viewing the CPU usage of SPOOLSV

- Check the free space on the drive hosting the spooler file, and change its destination (see Figure 16-7). The amount of free space needed for the spooler file is determined by the size and number of your print jobs and the settings of the logical printer; typically, 100 MB is sufficient. You should change the spool file host drive if there is insufficient space or if you suspect that the drive is not performing fast enough. This change is made on the Advanced tab of the Server Properties dialog box, accessed from the File menu of the Printers folder. See Chapter 10 for more information.

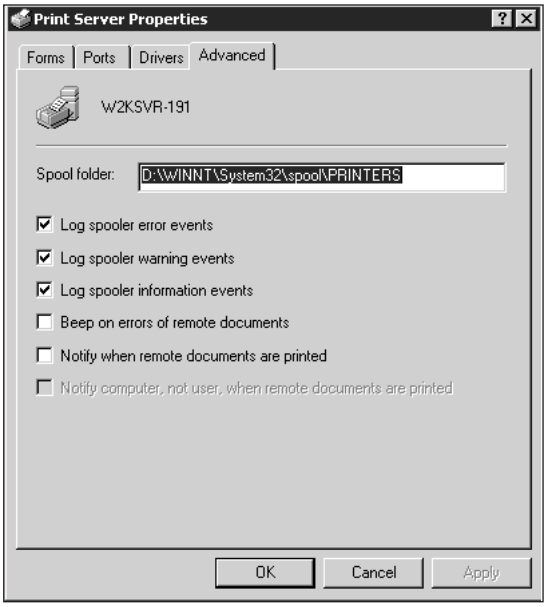

Figure 16-7 The Advanced tab of the Printer Server Properties dialog box, showing the spool folder

Table 16-1 summarizes some common network printing problems and their solutions.

Table 16-1 Printer Troubleshooting

Network Printing Problem	Solutions
Pages print, but only a single character appears on each page. —or— Pages print but they include the control codes in the document. —or— Pages print, but they show random characters instead of the desired document.	1. If the print job has not completed printing, delete it from the print queue to prevent wasting more paper. 2. Configure the printer to "Hold mismatched documents" (printer Properties dialog box, Advanced tab). 3. Remove and reinstall the logical printer and/or the printer driver on the client (if only a single workstation experiences the problem) or on the server (if all workstations experience the problem). 4. Verify that the data type set in the logical printer is correct for the application used, printer driver installed, and capabilities of the physical print device. 5. Stop and restart the Print Spooler service.

Table 16-1 Printer Troubleshooting (continued)

Network Printing Problem	Solutions
An access denied or no access available message is displayed when a print job is submitted.	This is typically caused by improper permissions defined on the printer share. Double-check the permission settings. You may also need to review the group memberships of the affected users if you are employing any Deny permissions on the printer share.
A network-attached printer shows an error light on the network interface.	A network communication or identification error has occurred. Cycling the power on the printer may resolve the problem. If not, try disconnecting then reconnecting the network media while the printer is powered off.
No documents are being created by the physical print device, but the print queue shows that the print job is printing.	1. View the print queue to see if a print job is stalled or paused. If so, delete or resume the print job. 2. If no other print job is present, delete the current print job and resubmit it from the original application. 3. Stop and restart the Print Spooler service.
The printer share is not visible from a client (that is, it does not appear in Network Neighborhood or My Network Places).	1. The client system may not be properly connected to the network. Shut down the client, check all physical network connections, and reboot. Test to see if you can access any other network resources. 2. Check the installed protocol and its settings, especially if TCP/IP is being used. 3. Check the domain/workgroup membership of the client.
On larger print jobs, pages from the end of the print job are missing from the printed document.	This can occur when insufficient space is available on the drive hosting the spooler file. Either free up space on the host drive or move the spooler file to a drive with more available space.

This section covers most of the more common print-related problems. To start step-by-step printer troubleshooting, try Hands-on Project 16-4. For more tips on printer troubleshooting, consult the *Windows 2000 Resource Kit*.

Troubleshooting RAS Problems

Remote Access Service (RAS) is another area with numerous possible points of failure—from the configuration of the computers on both ends, to the modem settings, to the condition of the communications line. Unfortunately, there is no ultimate RAS troubleshooting guide, but here are some solid steps in the right direction:

- Check all physical connections.

- Check the communications line itself, with a phone if appropriate.
- Verify the RAS configuration and the modem setup. To verify these items, attempt to establish a connection to another server or delete and re-create the connection object. For detailed examples and hands-on projects for this subject, see Chapter 9.
- Check that the client and the server dial-up configurations match, including speed, protocol, and security (see Figure 16-8 for an example of the security settings for a dial-up connection. You'll need to view the other tabs to compare and confirm speed, protocol, and other connection settings).

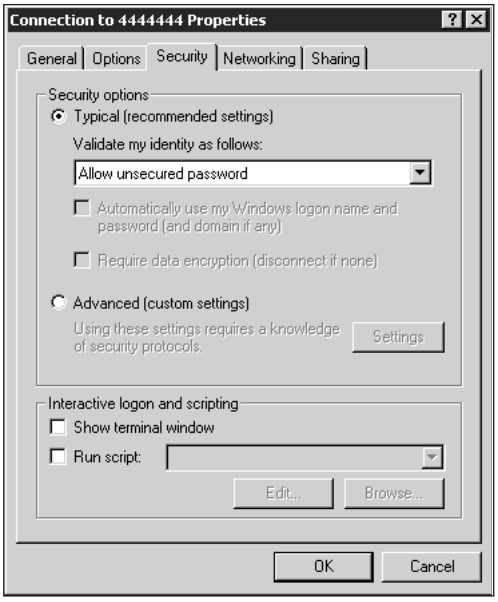

Figure 16-8 The Security tab of the Properties dialog box of a Connection object

- Verify that the user account has RAS privileges.
- Inspect the RAS-related logs: Device.log and Modemlog.txt. Look for errors involving failure to connect, failure to dial, failure to authenticate, failure to negotiate encryption, failure to establish a common protocol, and link termination.
- Remember that Multilink and callback will not work together. You must select one or the other. Figure 16-9 shows a configuration setting on a connection object that allows the caller to define the callback number.
- Autodial and persistent connections may cause the computer to attempt RAS connection at logon.

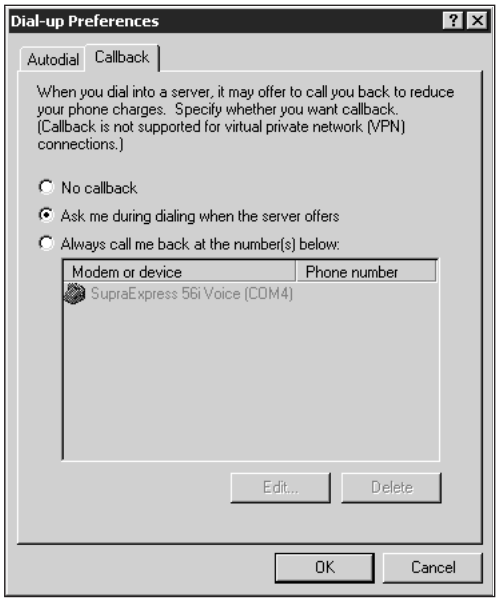

Figure 16-9 The Callback tab of the Dial-up Preferences dialog box

Table 16-2 outlines common RAS problems and solutions.

Table 16-2 RAS Troubleshooting

RAS Problem	Solutions
The connection object fails to establish a network link with the remote server.	1. Check the username, password, and phone number. 2. Verify that the modem device is powered on and properly connected to the computer and the phone line. You should also check the installed driver and update it if necessary. 3. Verify that the security settings match those required by the remote server. 4. Verify that the protocol settings match those required by the remote server.
The client has Multilink enabled and has three identical modems for the connection, but only a single modem establishes a network link with the remote server.	1. Verify that the remote server supports Multilink and that it has Multilink connections enabled. 2. Verify that you need to dial the same, or different, phone numbers when establishing a Multilink connection. 3. Cycle the power on the modems. Verify that they are properly attached to the computer and the telephone line.

Table 16-2 RAS Troubleshooting (continued)

RAS Problem	Solutions
A network link is broken during a remote session after a successful link is established.	1. Your phone line probably has call waiting, and another call came in. Disable call waiting via the connection object. 2. Your telephone line quality is poor, as is the case when old wiring is present, when phone lines pass by electrical interference, or when the weather is bad. You may need to upgrade your internal wiring, request a service upgrade from the telephone company, reroute wiring to avoid interference, or wait until the weather clears. 3. Remote systems can disconnect you for a variety of reasons, most beyond your control and knowledge. In most cases, simply try to reestablish the connection.

Most RAS problems are related to misconfiguration. For more details on RAS, refer to Chapter 9 or the *Windows 2000 Resource Kit*.

Troubleshooting Network Problems

Network problems can range from faults in the network cables or hardware, to misconfigured protocols, to workstation or server errors. As with other troubleshooting, attempt to eliminate the obvious and easy possibilities (such as physical connections and permissions) before moving on to more drastic, complex, or unreliable measures (IP configuration, routing, and domain structure). Cabling, connections, and hardware devices are just as suspect as the software components of networking.Verifying hardware functionality involves more than just looking at it; you may need to perform some electrical tests, change physical settings, or update drivers/ROM BIOS.

Some common-sense first steps you can take include:

- Check to see if other clients, servers, or subnets are experiencing the same problem.
- Check physical network connections, including the NIC, media cables, terminators, and logically proximate network devices (such as hubs, repeaters, and routers).
- Check protocol settings.
- Reboot the system.
- Verify that the NIC drivers are properly installed. Use the self-test or diagnostic tools or software for the NIC if available.
- Verify the domain/workgroup membership of the client.

Table 16-3 shows some common connectivity problems and their solutions.

Table 16-3 Network Connection Troubleshooting

Connectivity Problem	Solutions
The client does not seem to connect to the network (that is, no objects are visible in the Network Neighborhood). —or— The client is unable to be authenticated by the domain.	1. Use the Event Viewer to look for errors in the System log. Resolve any issues discovered. 2. Check the physical network connections, including the NIC, media, and local network devices. 3. Check the NIC driver, and update or replace it, if necessary. 4. Check the installed protocol and its configuration settings. 5. Check the domain/workgroup membership. 6. Reboot the client.
A system disconnects from the network randomly or when other computers boot onto the network.	1. Check to see that you are not violating the length, segments, or nodes per segment limitations on the network media in use. 2. Verify that all systems have unique address assignments and system computer names. 3. Check for breaks in the network media or the proximity of electrical or magnetic interference.
Shared network resources, such as folders and printers, cannot be accessed from a client.	1. Check the assigned permissions on the share itself and on the object (if applicable). 2. Check group memberships, if any Deny permissions are used. 3. Attempt to access the resources by using a different user account or client. 4. Check that the computer is connecting to the network.

Troubleshooting Disk Problems

The component on your computer that experiences the most activity is the hard drive, even more so than your keyboard and mouse. It should not be surprising that hard drive failures are common. Windows 2000 is natively equipped to maintain the file system (see Chapter 4), but even a well-tuned system is subject to hardware glitches. Most partition, boot sector, and drive configuration faults can be corrected or recovered from by using the Disk Management tool from the Computer Management utility of Administrative Tools (see Figure 16-10). However, the only reliable means of protecting data on storage devices is to maintain an accurate and timely backup, as discussed in Chapter 15. For detailed examples and information on using the Disk Management tool and troubleshooting disk problems, see Chapter 4.

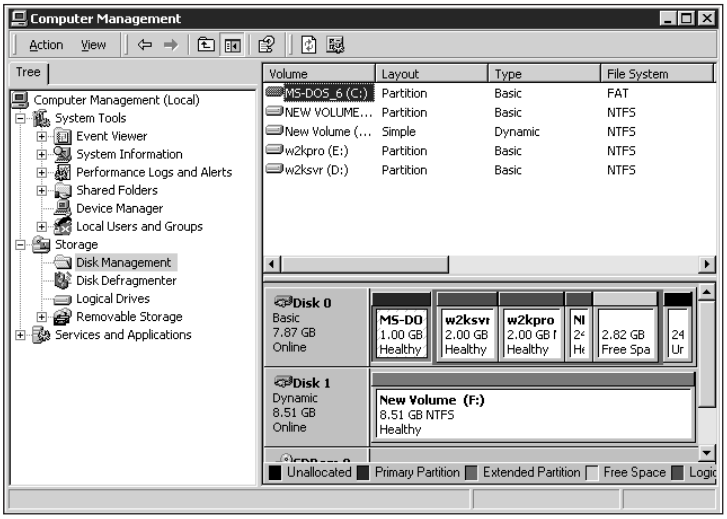

Figure 16-10 Disk Management tool from the Computer Management interface

Miscellaneous Troubleshooting Issues

There are several troubleshooting tips that don't fit into the other categories described in this chapter. They are included here.

Permission Problems

Permission problems (problems with accessing or managing system resources such as folders, files, or printers) usually occur when a user is a member of groups with conflicting permissions or when permissions are managed on a per-account basis. To test for faulty permission settings, attempt the same actions and activities with Administrator privileges (try Hands-on Project 16-5). Double-check a user's group memberships to verify that there are no Deny access settings causing the problem. This means examining the access control lists (ACLs) of the objects and the share, if applicable (see Figure 16-11).

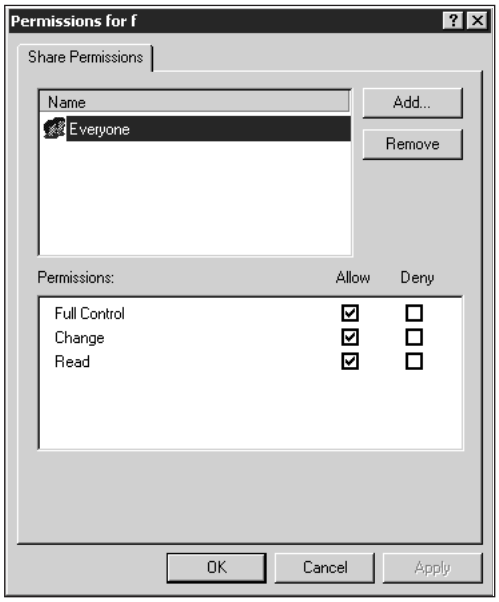

Figure 16-11 The Permissions dialog box for a share

It is important to remember that any changes to the access permissions of individual users or groups will not affect those users until the next time they log on. The access token used by the security system is rebuilt each time a user logs on.

Master Boot Record Problems

As you learned in Chapter 14, the master boot record (MBR) is the area of a hard drive that contains the data structure that initiates the boot process. If the MBR fails, the Emergency Repair Disk (ERD) cannot be used to repair it. Instead, you'll need to use a DOS 6.0+ bootable floppy disk and execute *FDISK /MBR* from the command prompt. This will re-create the drive's MBR and restore the system correctly. If you don't have access to DOS FDISK, you'll have to perform a complete install/upgrade of Windows 2000 to allow the setup routine to re-create the MBR. It may also be possible to use the Recovery Console fixmbr command to repair a corrupt master boot record.

Using the Dr. Watson Debugger

Windows 2000 has an application error debugger called **Dr. Watson**. This diagnostic tool detects application failures and logs diagnostic details. Data captured by Dr. Watson is stored in the Drwtsn32.log file. Dr. Watson can also be configured to save a memory dump of the application's address space for further investigation. However, the information extracted and stored by Dr. Watson is really only useful to a Microsoft technical professional who is well versed in the cryptic logging syntax used.

Windows 2000 automatically launches Dr. Watson when an application error occurs. To configure Dr. Watson, however, you'll need to launch it from the Start, Run command with *DRWTSN32*. Figure 16-12 shows the configuration dialog box for Dr. Watson.

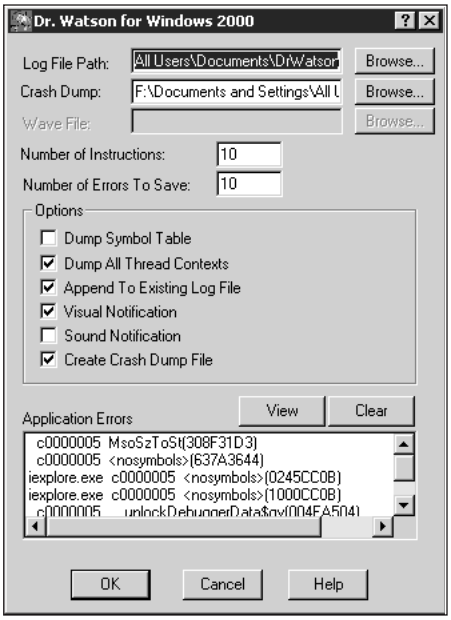

Figure 16-12 Dr. Watson

As you can see, this dialog box lists the configuration items for the following:

- The log file path, which is where the Dr. Watson log file is stored
- The crash dump, which provides the dump location for an application's virtual machine's address space
- The number of instructions and errors to record in log file
- Options for what to include in the log file and the way to notify the user of an application fault
- A list of previous application errors, with access to the log file details

Applying Service Packs and Hot Fixes

A **service pack** is a collection of code replacements, patches, error corrections, new applications, version improvements, and/or service-specific configuration settings from Microsoft that correct, replace, or hide the deficiencies of the original product or preceding service packs or hot fixes. A **hot fix** is similar to a service pack, except that it addresses only a single problem, or a small number of problems, and may not be fully tested.

You should apply a hot fix only if you are experiencing the problem it was created to fix, otherwise the hot fix may cause other problems.

Service packs are cumulative. For example, Service Pack 3 (SP3) for Windows NT 4.0 contains SP2 plus all post-SP2 hot fixes. Thus, the latest service pack is all you need to install. For instructions on installing and removing service packs, try Hands-on Projects 16-6 and 16-7.

At this writing, Microsoft has announced that it will release the first service pack for Windows 2000 by summer 2000. We crafted this section based on prerelease documentation and our experience with Windows NT service packs. Take the time to review the documentation included with the service pack once it is available.

It is a common practice among production networks to wait one to three months after the release of a new service pack before deploying it. This gives the installed community time to test and provide feedback about the patch. The track record of initial reliability of service packs is varied, so it's best to wait and verify reliability.

A few important points to remember about patches such as service packs and hot fixes include:

- Always make a backup of your system before applying any type of patch; this will give you a way to restore your system if the fix damages the OS.
- Be sure to retrieve a patch for the correct CPU type and language version.
- Always read the readme and Knowledge Base documents for each patch before installing it.
- Update your Emergency Repair Disk (ERD) both before and after applying a patch.
- Make a complete backup of the Registry, using the Registry Editor or the Regback utility from the *Windows 2000 Resource Kit*.
- Export the disk configuration data from Disk Administrator.
- Because service packs rewrite many system-level files, you must disconnect all current users, exit all applications, and temporarily stop all unneeded services before installing any service pack or patch.

To locate Microsoft Knowledge Base documents, visit or use one of these resources:

- Web site: *http://support.microsoft.com/*
- TechNet CD
- Microsoft Network

- CompuServe: GO MICROSOFT
- Resource Kit documentation (online help file)

Service packs and hot fixes can be retrieved from:

- Microsoft FTP site: *ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/*
- The Microsoft Windows Web site: *http://www.microsoft.com/windows/* (look for the download link)

To determine what service packs have been applied to your system, you can use one of the following techniques:

- Enter *WINVER* from a command prompt to view an About The System dialog box.
- Select Help, About Windows 2000 from the menu bar of any native tool such as Windows Explorer.
- Use the Registry Editor to view the *CSD Version* value in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion subkey.

Using Microsoft References for Troubleshooting

Several Microsoft resources are available to aid you in troubleshooting and working with Windows 2000:

- *Microsoft Web site: http://www.microsoft.com/windows/*
- *The Knowledge Base:* The predecessor to and a resource for the TechNet CD is the online Knowledge Base. This resource can be accessed by several means, which we detailed earlier in this chapter.
- *TechNet:* The best periodic publication from Microsoft is *TechNet*. This multi-CD collection is an invaluable resource for white papers, FAQs, troubleshooting documents, book excerpts, articles, and other written materials, plus utilities, patches, fixes, upgrades, drivers, and demonstration software. At only $300 per year (as of this writing), it is well worth the cost. It is also available online in a limited form at *http://www.microsoft.com/technet/*.
- *Resource Kits:* The Resource Kits (RKs) are useful information sources. These are available in electronic form through TechNet as a whole and through the online services in portions. RKs document material outside that contained in the manuals, and often include add-on software utilities to enhance product use.

CHAPTER SUMMARY

- Information is the most valuable tool for troubleshooting. Maintain a Computer Information File (CIF) and a detailed history log of troubleshooting activities.
- No matter what problems or errors are discovered on your computer system, there are several common-sense principles of troubleshooting that you should always follow. These include performing one task at a time, remaining calm, isolating the problem, and performing the simplest fixes first.
- The Windows 2000 tools most often used for troubleshooting are Event Viewer and the Computer Management tool.
- There are five common installation problems: media errors, domain controller communication difficulties. Stop message errors or halting on blue screen, hardware problems, and dependency failures.
- Printer problems are most often associated with physical configuration or spooling problems.
- RAS and network problems are caused by several types of problems, but the most common is misconfiguration.
- Service packs and hot fixes are used to repair portions of Windows 2000 after its release.
- Microsoft has provided several avenues to gain access to information about the operation and management of Windows 2000, including a substantial collection of troubleshooting documentation.

KEY TERMS

Application log — A log automatically created by Windows 2000 that records application events, alerts, and system messages.

computer information file (CIF) — A detailed collection of all information related to the hardware and software products that compose your computer (and even your entire intranet).

Dr. Watson — An application error debugger. This diagnostic tool detects application failures and logs diagnostic details.

Event Viewer — The utility used to view the three logs automatically created by Windows 2000: the System log, Application log, and Security log.

hot fix — Similar to a service pack, except that a hot fix addresses only a single problem, or a small number of problems, and may not be fully tested.

Security log — A log automatically created by Windows 2000 that records security-related events.

service pack — A collection of code replacements, patches, error corrections, new applications, version improvements, or service-specific configuration settings from Microsoft that correct, replace, or hide the deficiencies of the original product or preceding service packs or hot fixes.

System log — A log automatically created by Windows 2000 that records information and alerts about the Windows 2000 internal processes.

Review Questions

1. When approaching a computer problem, which of the following should you keep in mind? (Choose all that apply.)
   a. how the problem was last solved
   b. what changes were recently made to the system
   c. information about the configuration state of the system
   d. the ability to repeat the failure
2. If a media error occurs during installation, which of the following are steps you should take to eliminate the problem? (Choose all that apply.)
   a. Attempt to recopy or reaccess the file that caused the failure.
   b. Switch media sources or types.
   c. Open the Control Panel and reinstall the appropriate drivers.
   d. Restart the installation from the beginning.
3. Which of the following Windows 2000 repair tools can be used to gain information about drivers or services that failed to load?
   a. Event Viewer
   b. Registry
   c. System applet
   d. Dr. Watson
4. In addition to the Event Viewer and the System Information tool, which of the following are useful tools in troubleshooting? (Choose all that apply.)
   a. Advanced Options Boot Menu
   b. Registry editors
   c. backup software
   d. Time/Date applet
5. Your best tool in troubleshooting is:
   a. a protocol analyzer
   b. information
   c. administrative access
   d. redundant devices
6. Which of the following are possible troubleshooting techniques for eliminating printer problems? (Choose all that apply.)
   a. Check the physical aspects of the printer—cable, power, paper, toner, and so on.
   b. Check the print queue for stalled jobs.
   c. Attempt to print from a different application or a different client.
   d. Stop and restart the spooler, using the Services tool.

7. What is the most common cause of RAS problems?
   a. telco service failures
   b. misconfiguration
   c. user error
   d. communications device failure
8. A user's ability to access a resource is controlled by access permissions. If you suspect a problem with a user's permission settings, what actions can you take? (Choose all that apply.)
   a. Attempt the same actions and activities with the Administrator account.
   b. Delete the user's account and create a new one from scratch.
   c. Double-check group memberships to verify that no Deny access settings are causing the problem.
   d. Grant the user Full Access to the object directly.
9. What application automatically loads to handle application failures?
   a. Event Viewer
   b. System applet
   c. Computer Management
   d. Dr. Watson
10. If you are going to create a CIF, which of the following is the most important?
    a. Include the vendor's mailing address.
    b. Keep everything in electronic form.
    c. Update the contents often.
    d. Use nonremovable labels on all components.
11. Which of the following are important actions to perform before installing a service pack or a hot fix? (Choose all that apply.)
    a. Make a backup of your system.
    b. Read the readme and Knowledge Base documents.
    c. Make a complete backup of the Registry.
12. What are some common-sense approaches to troubleshooting? (Choose all that apply.)
    a. Understand TCP/IP routing table configuration.
    b. Know your system.
    c. Undo the last alteration to the system.
    d. Replace all server hardware when one device fails.
    e. Let the fault guide you.
13. You can often resolve problems or avoid them altogether if you take the time to write out a history or log of problems and both failed and successful solution attempts. True or False?

14. When installing a new Windows 2000 domain controller into an existing domain, you can experience communication problems with the current domain controller. After you've verified that the current domain controller is online and properly connected to the network, what other items should be considered as possible points of failure? (Choose all that apply.)
    a. administrative account name
    b. subnet mask
    c. password
    d. domain name
15. Blue screen or Stop errors often occur on a system containing one or more devices that are not found on the HCL. True or False?
16. If the driver for your network interface card fails, which other components of your system are most likely to fail due to dependency issues? (Choose all that apply.)
    a. network protocol
    b. Client Services for NetWare
    c. video driver
    d. WinLogon
17. Errors involving internal processes, such as hardware and operating system errors, warnings, and general information messages, are recorded in the Application log of the Event Viewer. True or False?
18. The best way to resolve a hardware problem during installation is to:
    a. Restart the installation from scratch without any other modifications.
    b. Press and hold the Ctrl key during the installation.
    c. Remove or replace the non-HCL hardware.
    d. Recopy the distribution files.
19. An event detail viewed from the Event Viewer's logs provides specific information on the time, location, user, service, and resolution for all encountered errors. True or False?
20. The Computer Management tool offers links to several important administrative and management utilities including: (Choose all that apply.)
    a. Control Panel
    b. Event Viewer
    c. Performance Monitor
    d. Local Security Policy
    e. Local Users and Groups
21. The Storage section of the Computer Management tool offers utilities to perform what types of operations? (Choose all that apply.)
    a. defragmentation
    b. partitioning

c. managing removable storage
d. compressing floppies

22. When a printer fails to output your documents, which of the following is a possible troubleshooting first step?
    a. replacing the printer
    b. restarting the spooler
    c. reinstalling the operating system
    d. deleting and re-creating the shared printer
23. Both printers and RAS connections can suffer from the most common problem: physical connection interruptions. True or False?
24. When a user complains about being unable to access a resource that other users of similar job descriptions are able to access, what should you consider when attempting to troubleshoot this issue? (Choose all that apply.)
    a. group memberships
    b. ACL on the object
    c. domain membership
    d. speed of network connection
25. When you alter the group memberships of a user, you need to perform what operation to ensure that the changes are taking effect?
    a. reboot the server
    b. enable auditing on file objects
    c. restart the messaging and alert services
    d. log the user account off, then have the user log back on

HANDS-ON PROJECTS

Project 16-1

To use the Event Viewer:

1. Open the Event Viewer from the Start menu (click **Start**, point to **Programs**, point to **Administrative Tools**, click **Event Viewer**).
2. Select the **System Log** from the list of available logs in the left pane.
3. Notice the various types of events that appear in the right pane.
4. Select an event in the right pane.
5. Select the **Action** menu, then **Properties**.
6. Review the information presented by the event detail. Try to determine on your own what types of errors, warnings, or information are presented in the detail and why the detail was created.
7. Click the up and/or down arrows to view other event details.

8. Click **OK** to close the event detail.
9. Close Event Viewer.

Project 16-2

To extract information for a CIF:

This hands-on project suggests a method to obtain some information about your system for a CIF; it does not constitute a complete or exhaustive collection of data. This activity is only one part of the task of creating a CIF.

1. Open the Control Panel (click **Start**, point to **Settings**, click **Control Panel**).
2. Double-click **Administrative Tools**.
3. Double-click **Computer Management**.
4. In the left pane, select **System Information** (see Figure 16-13) from within the Computer Management portion of the list.
5. Expand the **System Information** entry by clicking the boxed plus sign to the left of the node.
6. Take the time to expand and select each item within the System Information node hierarchy. As you view each page of data, consider the value of this data for future troubleshooting and decide whether to print or save the information.
7. To print a page, click the **Print** button in the toolbar.
8. To save a page, click on the **Save System Information File** or **Save Text Report** button in the toolbar.
9. When you have finished examining the System Information tool, close the Computer Management utility.

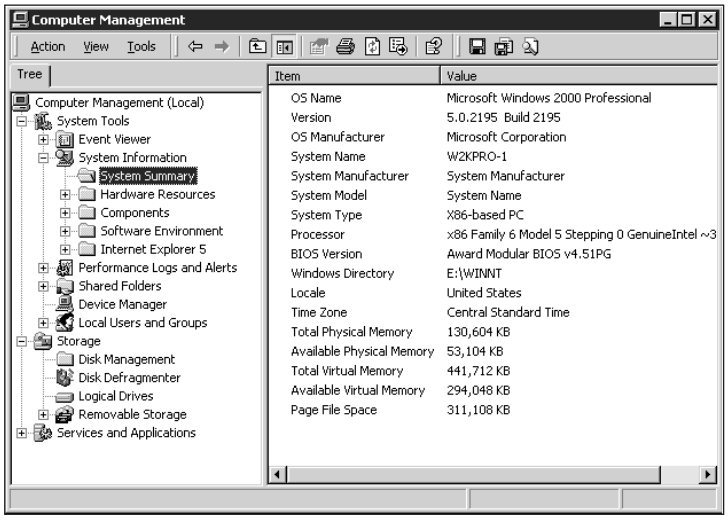

Figure 16-13 The System Information tool

Project 16-3

To explore the Computer Management utility:

1. Open the **Control Panel** (click **Start**, point to **Settings**, click **Control Panel**).
2. Double-click **Administrative Tools**.
3. Double-click **Computer Management**.
4. Notice that the left pane has three divisions: System Tools, Storage, and Services and Applications.
5. If necessary, expand the **System Tools** entry by clicking the boxed plus sign located to the left of the node name.
6. Explore the contents of the Event Viewer, System Information, Performance Logs and Alerts, Shared Folders, Device Manager, and Local Users and Groups sections by expanding them one at a time. To view the contents of any item, select it in the left pane so that its contents will be displayed in the right pane.
7. Once you've viewed the contents of the System Tools section, view the contents of the Storage section. This section includes Disk Management, Disk Defragmenter, Logical Drives, and Removable Storage.
8. Once you've viewed the contents of the Storage section, view the contents of the Services and Applications section. The items in this section vary based on installed applications and services but can include Telephony, WMI Control, Services, and Indexing Service.
9. Once you've viewed the contents of the Services and Applications section, close the Computer Management utility.

Project 16-4

To troubleshoot a printer problem:

This hands-on project is not an exhaustive process for printer troubleshooting; it includes some of the actions that may be required to resolve a printer problem.

1. First, check that the printer is online and has power, paper, and toner. Check the printer's own error-reporting center (often a light or an LCD) for any possible hardware errors.
2. Open the Printers applet (click **Start**, point to **Settings**, click **Printers**).
3. To display the printer queue window, double-click the installed printer that you suspect is having a problem.
4. If any documents appear in the printer queue window, select the topmost document, then select **Document**, **Restart**.
5. If the printer still fails to function, go to the Control Panel (click **Start**, point to **Settings**, click **Control Panel**).

6. Double-click the **Administrative Tools** icon.
7. Double-click **Computer Management**.
8. Drill down in the hierarchy in the left pane to locate and select the Services tool (**Computer Management**, **Services and Applications**, **Services**).
9. Locate and select the **Print Spooler** service (see Figure 16-14).

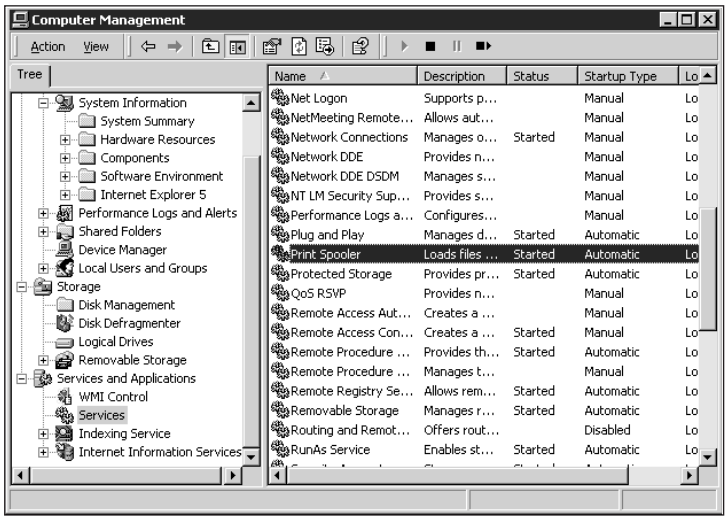

Figure 16-14 The Print Spooler service as seen through the Services tool

10. Select **Action**, **Stop**.
11. Select **Action**, **Start**.
12. Close the Computer Management utility.
13. Close the Control Panel.
14. If the printer still fails to function, return to the Printer queue window that was left open.
15. Select the topmost document in the printer queue.
16. Click the **Document** menu, then select the **Cancel** command to remove the print job from the queue.
17. If this was the only print job in the queue, print another document. If this was not the only print job in the queue, wait to see if the remaining print jobs print.
18. Close the Printer queue.

Consult Chapter 10 for more details on managing and troubleshooting printing.

Project 16-5

To troubleshoot permission problems:

This hands-on project is not an exhaustive process for permission troubleshooting; it includes only some of the actions that may be required to resolve permission problems.

1. If a user cannot access a resource to which they should have access, first reboot their system (**Start**, **Shutdown**). Select **Restart** from the drop-down menu, then click **OK**.
2. After rebooting, log back on as the user. Test to see if you can access the resource.
3. If the resource is still not accessible, log off and log back on as an administrator. Press **Ctrl+Alt+Delete** at the logon prompt, provide the user account name for the administrator and the associated password, and click **OK**.
4. Once logged on as the administrator, attempt to access the resource. If the resource can be accessed, the problem is with the assigned permissions for the user account. Most likely the user account is not a member of the proper group or is a member of a group that has Deny access set for that resource.
5. If the resource cannot be accessed by the administrator, the problem may lie with the system. This could include network communications, domain membership, or corrupted system drivers and files. You will need to troubleshoot these other possible causes of the problem.
6. If you discover that group membership is the problem, make the appropriate group membership changes, then force the user to log off, then log back on (changes do not take effect until the next logon).

Project 16-6

To apply a service pack:

1. Move or copy the service pack (SP) file into an empty directory as follows: from within Windows Explorer, create a new directory on a volume with at least 100 MB of free space (more may be required depending on the size of the service pack). Move or copy the SP into the new empty directory.
2. Close all applications, especially debugging tools, virus scanners, and any other non-Microsoft or third-party tools.
3. Locate and execute **Update.exe** with the **Start**, **Run** command.
4. Follow any prompts that appear. If you want the ability to uninstall the service pack, be sure to select the option to store uninstall information. It's generally a good idea to select this option.
5. When instructed, reboot your system.
6. After rebooting, you can delete the service pack files and the temporary directory from your hard drive (refer to Step 1).

Project 16-7

To uninstall a service pack:

You must have selected the "save uninstall information" option during the initial application of the service pack in order to uninstall it.

1. Extract the original SP archive into an empty directory. If you retained the SP archive and temporary directory from the installation procedure, you do not need to repeat this activity.
2. Locate and execute **Update.exe**.
3. Follow the prompts that appear.
4. Click the **Uninstall a previously installed service pack** button.
5. Follow the prompts.
6. Reboot.

Project 16-8

To verify that the Workstation and Server services are started after bootup:

1. Open the **Control Panel** (click **Start**, point to **Settings**, click **Control Panel**).
2. Double-click **Administrative Tools**.
3. Double-click **Computer Management**.
4. Expand the **Services and Applications** section by clicking on the boxed plus sign next to the node name, if it is not already expanded.
5. Select the **Services** object.
6. Scroll down in the right pane to locate the Workstation service.
7. Notice the item in the Status column. If it says "Started," then you can skip to Step 9.
8. If the Status column is blank for the Workstation service, it failed to launch at startup. You can attempt to launch the service by selecting it, then clicking the Action menu, then clicking on Start.
9. Scroll down in the right pane to locate the Server service.
10. Notice the item in the Status column. If it says "Started," then you can skip to Step 12.
11. If the Status column is blank for the Server service, it failed to launch at startup. You can attempt to launch the service by selecting it, then clicking the Action menu, then clicking on Start.
12. Close the Computer Management console.

CASE PROJECTS

1. After installing a new drive controller and a video card, along with their associated drivers, Windows 2000 refuses to boot, and booting with the Last Known Good Configuration (LKGC) option does not result in an operational system.

   Required result:

   - Return the system to a bootable and operational state.

   Optional desired results:

   - Retain the Security ID.
   - Retain most, if not all, of the system's configuration.

   Proposed solution:

   Perform a complete reinstallation of Windows 2000.

   Indicate which of the following occurs, and explain why.

   a. The proposed solution produces the desired result and produces both of the optional desired results.

   b. The proposed solution produces the desired result, but only one of the optional desired results.

   c. The proposed solution produces the desired result, but neither of the optional desired results.

   d. The proposed solution does not produce the desired result.

2. After installing a new drive controller and a video card, along with their associated drivers, Windows 2000 refuses to boot and the LKGC does not result in an operational system.

   Required result:

   - Return the system to a bootable and operational state.

   Optional desired results:

   - Retain the Security ID.
   - Retain most, if not all, of the system's configuration.

   Proposed solution:

   Perform an upgrade reinstallation of Windows 2000.

   Indicate which of the following occurs, and explain why.

   a. The proposed solution produces the desired result and produces both of the optional desired results.

   b. The proposed solution produces the desired result, but only one of the optional desired results.

   c. The proposed solution produces the desired result, but neither of the optional desired results.

   d. The proposed solution does not produce the desired result.

3. Describe the common problems associated with installing Windows 2000 and the steps to take to either avoid these problems or resolve them.